

How to configure Google Cloud Identity as a Chronicle IdP

How-to guide

Requirements

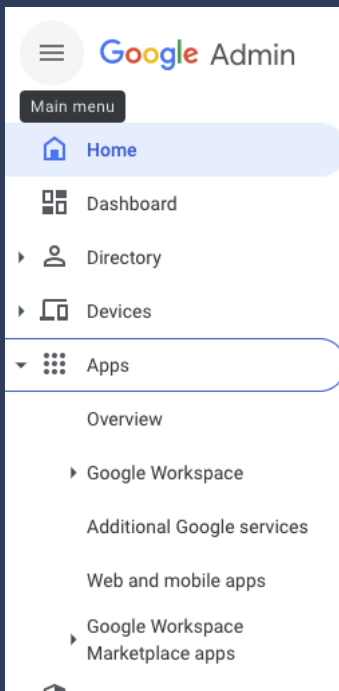
- You will need an account with access to the Google admin portal, and the rights to create an app
- You will need an account to login to Chronicle

Overview

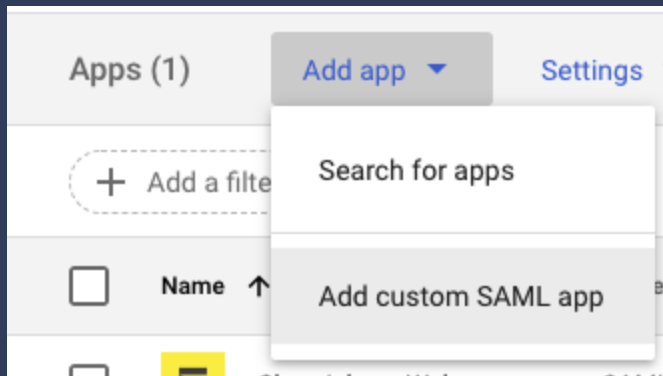
This document describes the process for integrating Google Cloud Identity into Chronicle to provide single sign-on (SSO) capabilities for you and your organization.

Creating the SAML Application

1. Login to your Google Admin console at <https://admin.google.com>.
2. Under the main menu, select **Apps > Web and mobile apps**



3. Click **Add app > Add custom SAML app**



4. Complete **App name**, **Description**, and add an **App icon** if you wish, then click **Continue**.

A screenshot of the 'Add custom SAML app' wizard in the Google Admin console. The wizard has four steps: 1. App details, 2. Google Identity Provider details, 3. Service provider details, and 4. Attribute mapping. Step 1 is currently active. The 'App details' section includes a text input for 'App name' with the value 'Google Chronicle', a text input for 'Description', and an 'App icon' section with a camera icon and the text 'Attach an app icon. Maximum upload file size: 4 MB'. At the bottom right, there are 'CANCEL' and 'CONTINUE' buttons.

5. Click **Continue** again on the **Google Identity Provider details** page.

Add custom SAML app

App details
Google Identity Provider detail:
Service provider details
Attribute mapping

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. [Learn more](#)

Option 1: Download IdP metadata

DOWNLOAD METADATA

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

https://accounts.google.com/o/saml2/ldp?idpid=C00jd0ttc

Entity ID

https://accounts.google.com/o/saml2/ldp=C00jd0ttc

Certificate

Google_2026-8-26-12756_SAML2_0
Expires Aug 26, 2026

—BEGIN CERTIFICATE—
MIIDdCCAlYgAwIBAgIwGAxGuQh9MA0GCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSBjb2dsZSBGb3IgV29yazELMAKGA1UEBhMCVVMxEzARBgNVBAgTCkNhbm3JuaWEwHhcNMjEwODI3

SHA-256 fingerprint

6. On the **Service provider details** page, under **ACS URL** enter the ACS callback URL provided by Google on setting up your instance, this will be in the format: https://myinstance.backstory.chronicle.security/acs, and under **Entity ID**, enter the URL for your instance in this format: https://myinstance.backstory.chronicle.security/. Click **Continue**.

×

Add custom SAML app

✓ App details

✓ Google Identity Provider details

3 Service provider details

4 Attribute mapping

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL

ACS URL is required

Entity ID

Entity ID is required

Start URL (optional)

☐ Signed response

Name ID

Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format

UNSPECIFIED

Name ID

Basic Information > Primary email

7. On this final page, click **Finish** to complete the app creation process.

×

Add custom SAML app

✓ App details

✓ Google Identity Provider details

✓ Service provider details

4 Attribute mapping

BETA

Technical support and audit logs won't be available for items marked Beta.

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes

App attributes

ADD MAPPING

Group membership (optional)

BETA

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

Google groups

App attribute

Search for a group

→

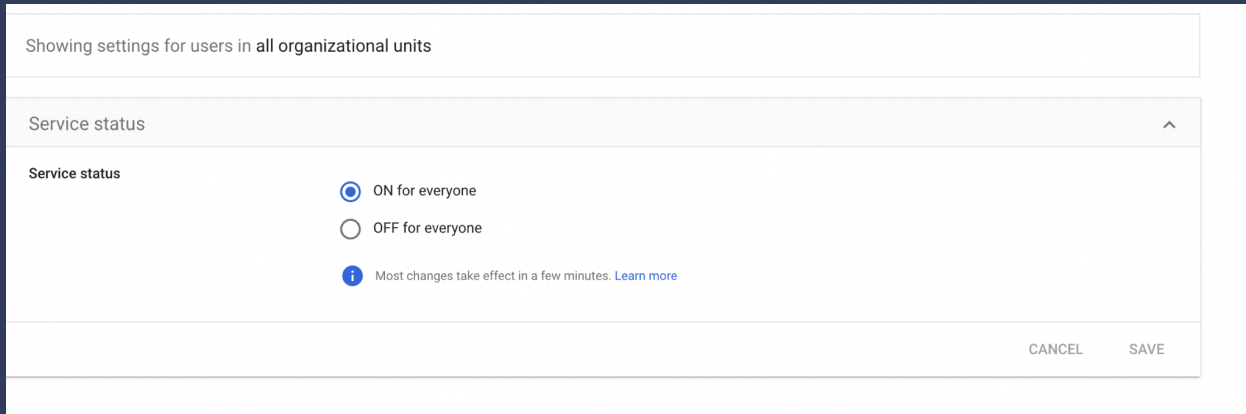
Groups

BACK

CANCEL

FINISH

8. If you click **User access**, you can add users, Organizational Units or otherwise configure who can access your SAML application




Showing settings for users in all organizational units

Service status

Service status

☒ ON for everyone

☐ OFF for everyone

 Most changes take effect in a few minutes. [Learn more](#)

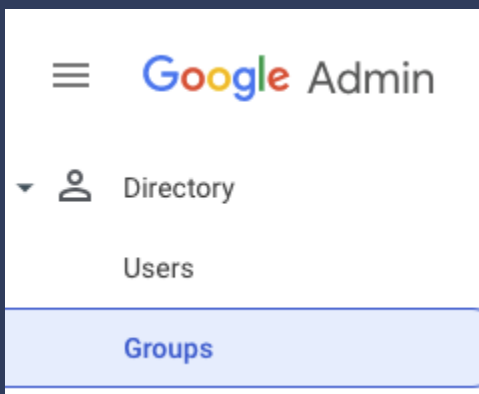
CANCEL SAVE

9. Now we can download the application metadata XML file by going to **Apps > Web and mobile apps**, selecting your application, and clicking the **Download Metadata** button.

Integrating Okta groups with RBAC (Optional)

RBAC in Chronicle provides [a number of possible roles](#), you can create Google groups for each of these roles, or just a subset. For the sake of this document, we are just going to use **Admin**, **Editor**, and **Viewer** groups and roles.

If the groups you wish to use for mapping don't already exist, then go to **Directory > Groups** and create them.



Go to your SAML application, and click on the **SAML attribute mapping** section. Under **Group membership (optional)** search for and select each of the groups you want to access the application, and set **App** attribute to **group**, once done click **Save**.

SAML attribute mapping

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. [Learn more](#)

Google Directory attributes

App attributes

ADD MAPPING

Group membership (optional) BETA

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

Google groups

Chronicle Admin

Chronicle Editor

Chronicle Viewer

Search for a group

App attribute

→ group


CANCEL

SAVE

Configuring Chronicle

After providing the metadata XML file generated earlier, you will be able to login to your Chronicle instance using your Google identity, via the URL provided by Google. You can now configure RBAC using either groups or users as follows:

1. Login to Chronicle
2. Click the menu icon in the top right corner of the UI



3. Select **Settings**, you will see your Profile appear. If you added group claims to your SAML application then you should see the passed groups here (if you did add group claims but don't see the groups listed then double check your SAML application configuration and raise a ticket with Chronicle support if you still cannot see the groups).
4. Click **Users & Groups** in the left hand menu, this will display any users or groups configured with explicit permissions in your system.
5. Follow the instructions [here](#) to add/remove users or groups and map them to the relevant permissions.
6. If you want to, and once you have completed the above steps, you can change the default permission through the dropdown in the top right hand corner of this window:

New and unassigned users/groups will default to role: Viewer